

# **Отчёт по лабораторной работе 16**

**Базовая защита от атак типа «brute force»**

Авдадаев Джамал Геланиевич

# **Содержание**

<b>1 Введение</b>	<b>5</b>
1.1 Цель работы . . . . .	5
<b>2 Процесс работы</b>	<b>6</b>
2.1 Установка и запуск Fail2ban . . . . .	6
2.1.1 Установка Fail2ban . . . . .	6
2.1.2 Просмотр журнала Fail2ban . . . . .	6
2.1.3 Создание локального файла конфигурации и включение за- щиты SSH . . . . .	7
2.1.4 Включение защиты HTTP-сервисов . . . . .	9
2.1.5 Включение защиты почтовых сервисов . . . . .	11
2.2 Проверка работы Fail2ban . . . . .	13
2.3 Внесение изменений во внутреннее окружение виртуальной машины	17
<b>3 Итоги</b>	<b>18</b>
3.1 Вывод . . . . .	18
3.2 Контрольные вопросы . . . . .	18

# Список иллюстраций

2.1 Установка и запуск fail2ban . . . . .	6
2.2 Просмотр журнала Fail2ban . . . . .	7
2.3 Локальная конфигурация Fail2ban SSH . . . . .	8
2.4 Создание и запуск jail-ов SSH . . . . .	9
2.5 Включение HTTP-jail-ов . . . . .	10
2.6 Работа HTTP-jail-ов . . . . .	11
2.7 Включение защиты почтовых сервисов . . . . .	12
2.8 Работа почтовых jail-ов . . . . .	13
2.9 Общий статус Fail2ban . . . . .	13
2.10 Статус защиты SSH . . . . .	14
2.11 Установка maxretry . . . . .	14
2.12 Блокировка IP после неудачных попыток входа . . . . .	15
2.13 Разблокировка адреса клиента . . . . .	15
2.14 Добавление ignoreip . . . . .	16
2.15 Fail2ban игнорирует IP-адрес клиента . . . . .	16
2.16 Создание каталогов и копирование конфигурации . . . . .	17
2.17 Скрипт protect.sh . . . . .	17

# **Список таблиц**

# **1 Введение**

## **1.1 Цель работы**

Получить навыки работы с программным средством Fail2ban для обеспечения базовой защиты от атак типа «brute force».

## 2 Процесс работы

### 2.1 Установка и запуск Fail2ban

#### 2.1.1 Установка Fail2ban

На сервер был установлен пакет fail2ban с помощью менеджера пакетов DNF. После завершения установки система вывела сообщение о том, что все необходимые компоненты были успешно добавлены.

```
Installed:
  fail2ban-1.1.0-6.el10_0.noarch          fail2ban-firewalld-1.1.0-6.el10_0.noarch      fail2ban-selinux-1.1.0-6.el10_0.noarch
  fail2ban-sendmail-1.1.0-6.el10_0.noarch

Complete!
[root@server.dgavdadaev.net server]# systemctl start fail2ban.service
[root@server.dgavdadaev.net server]# systemctl enable fail2ban.service
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' → '/usr/lib/systemd/system/fail2ban.service'.
[root@server.dgavdadaev.net server]#
```

Рис. 2.1: Установка и запуск fail2ban

Сервис Fail2ban был запущен и включён в автозагрузку.

Система создала символьную ссылку в директории `multi-user.target.wants`, подтверждающую успешную активацию сервиса.

#### 2.1.2 Просмотр журнала Fail2ban

Для проверки работы Fail2ban был открыт журнал событий.

Записи в логе показывают:

- запуск серверной части Fail2ban;

- запуск наблюдателя;
- подключение к базе данных;
- создание новой базы при первом запуске.

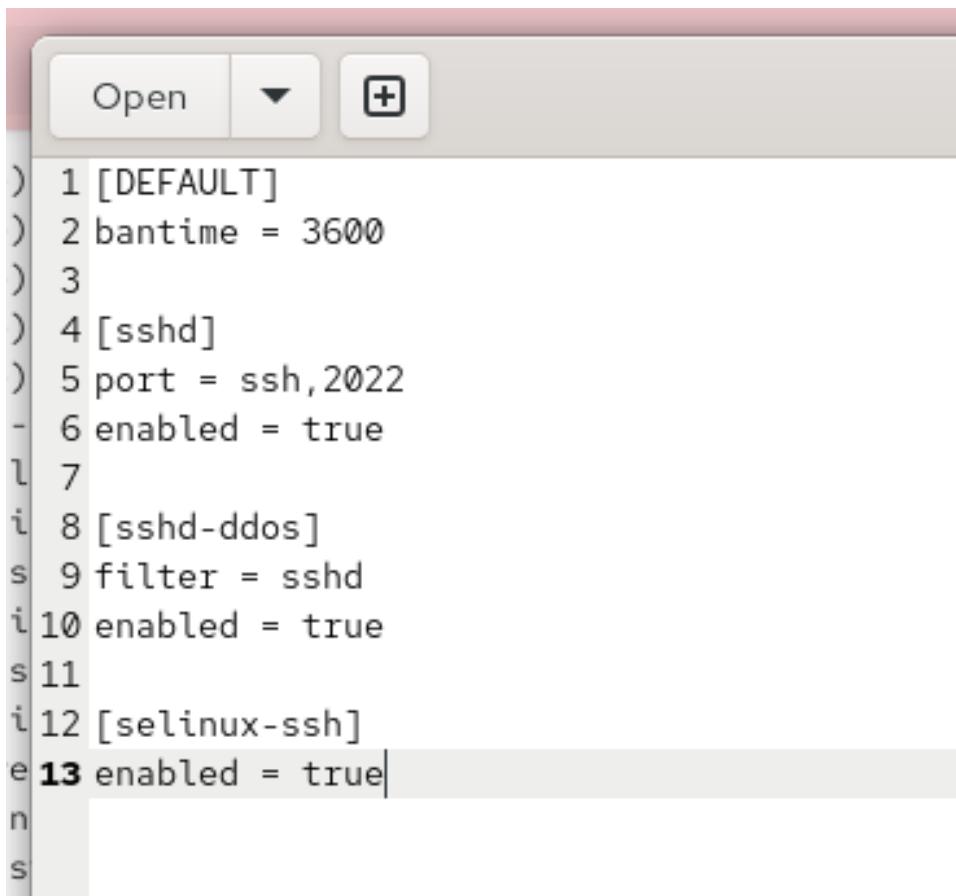
```
[dgavdadaev@server dgavdadaev.net ~]$ sudo tail -f /var/log/fail2ban.log
[sudo] password for dgavdadaev:
[17953]: INFO  -----
2025-12-11 11:15:41,470 fail2ban.server      [17953]: INFO  Starting Fail2ban v1.1.0
2025-12-11 11:15:41,470 fail2ban.server      [17953]: INFO  Observer start...
2025-12-11 11:15:41,470 fail2ban.database    [17953]: INFO  Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sq
liteDatabase'
2025-12-11 11:15:41,474 fail2ban.database    [17953]: WARNING New database created. Version '4'
```

Рис. 2.2: Просмотр журнала Fail2ban

### **2.1.3 Создание локального файла конфигурации и включение защиты SSH**

Для хранения индивидуальных настроек создан файл в jail.d.

В него добавлены параметры блокировки и включена защита SSH, включая несколько jail-ов для разных типов атак.



The screenshot shows a terminal window with a light gray background. At the top, there is a toolbar with three buttons: 'Open' (with a downward arrow), a dropdown menu, and a '+' button. The main area of the terminal contains the following configuration text:

```
) 1 [DEFAULT]
) 2 bantime = 3600
)
) 3
) 4 [sshd]
) 5 port = ssh,2022
) 6 enabled = true
l
7
i 8 [sshd-ddos]
s 9 filter = sshd
i 10 enabled = true
s 11
i 12 [selinux-ssh]
e 13 enabled = true|
n
s
```

Рис. 2.3: Локальная конфигурация Fail2ban SSH

После перезапуска Fail2ban в журнале появились записи о создании и запуске jail-ов:

- sshd;
- selinux-ssh;
- sshd-ddos.

Все jail-ы корректно активировались и начали обработку данных журналов.

```

2025-12-11 11:19:41,577 fail2ban.server      [18784]: INFO  Starting Fail2ban v1.1.0
2025-12-11 11:19:41,577 fail2ban.observer    [18784]: INFO  Observer start...
2025-12-11 11:19:41,577 fail2ban.database    [18784]: INFO  Connected to fail2ban persistent database '/var/lib/fail2ban/fail2ban.sq
lite3'
2025-12-11 11:19:41,578 fail2ban.jail       [18784]: INFO  Creating new jail 'sshd'
2025-12-11 11:19:41,580 fail2ban.jail       [18784]: INFO  Jail 'sshd' uses systemd {}
2025-12-11 11:19:41,582 fail2ban.jail       [18784]: INFO  Initiated 'systemd' backend
2025-12-11 11:19:41,584 fail2ban.filter     [18784]: INFO  maxlines: 1
2025-12-11 11:19:41,585 fail2ban.filtersystemd [18784]: INFO  [sshd] Added journal match for: '_SYSTEMD_UNIT=sshd.service + _COMM=sshd
+ _COMM=sshd-session'
2025-12-11 11:19:41,585 fail2ban.filter     [18784]: INFO  maxRetry: 5
2025-12-11 11:19:41,585 fail2ban.filter     [18784]: INFO  findtime: 600
2025-12-11 11:19:41,585 fail2ban.actions   [18784]: INFO  banTime: 3600
2025-12-11 11:19:41,585 fail2ban.filter     [18784]: INFO  encoding: UTF-8
2025-12-11 11:19:41,585 fail2ban.jail       [18784]: INFO  Creating new jail 'selinux-ssh'
2025-12-11 11:19:41,585 fail2ban.jail       [18784]: INFO  Jail 'selinux-ssh' uses pyinotify {}
2025-12-11 11:19:41,588 fail2ban.jail       [18784]: INFO  Initiated 'pyinotify' backend
2025-12-11 11:19:41,589 fail2ban.jail       [18784]: INFO  date pattern '': 'Epoch'
2025-12-11 11:19:41,589 fail2ban.filter     [18784]: INFO  maxRetry: 5
2025-12-11 11:19:41,589 fail2ban.filter     [18784]: INFO  findtime: 600
2025-12-11 11:19:41,589 fail2ban.actions   [18784]: INFO  banTime: 3600
2025-12-11 11:19:41,589 fail2ban.filter     [18784]: INFO  encoding: UTF-8
2025-12-11 11:19:41,590 fail2ban.filter     [18784]: INFO  Added logfile: '/var/log/audit/audit.log' (pos = 0, hash = 0447f9c83b285
4572b04db6490lee8578605c7dd)
2025-12-11 11:19:41,590 fail2ban.jail       [18784]: INFO  Creating new jail 'sshd-ddos'
2025-12-11 11:19:41,590 fail2ban.jail       [18784]: INFO  Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:19:41,591 fail2ban.jail       [18784]: INFO  Initiated 'pyinotify' backend
2025-12-11 11:19:41,591 fail2ban.filter     [18784]: INFO  maxlines: 1
2025-12-11 11:19:41,591 fail2ban.filter     [18784]: INFO  maxRetry: 5
2025-12-11 11:19:41,591 fail2ban.filter     [18784]: INFO  findtime: 600
2025-12-11 11:19:41,591 fail2ban.actions   [18784]: INFO  banTime: 3600
2025-12-11 11:19:41,591 fail2ban.filter     [18784]: INFO  encoding: UTF-8
2025-12-11 11:19:41,591 fail2ban.jail       [18784]: INFO  Jail 'sshd' started
2025-12-11 11:19:41,592 fail2ban.jail       [18784]: INFO  Jail 'selinux-ssh' started
2025-12-11 11:19:41,592 fail2ban.jail       [18784]: INFO  Jail 'sshd-ddos' started
2025-12-11 11:19:41,592 fail2ban.filtersystemd [18784]: INFO  [sshd] Jail is in operation now (process new journal entries)

```

Рис. 2.4: Создание и запуск jail-ов SSH

## 2.1.4 Включение защиты HTTP-сервисов

В локальный файл конфигурации были добавлены HTTP-jail-ы для защиты Apache от различных типов атак.

```
i 5 filter sshd
t 10 enabled = true
e 11
n 12 [selinux-ssh]
s 13 enabled = true
n 14
s 15 [apache-auth]
n 16 enabled=true
s 17
s 18 [apache-badbots]
s 19 enabled=true
n 20
n 21 [apache-noscript]
22 enabled=true
a 23
i 24 [apache-overflows]
i 25 enabled=true
26
l 27 [apache-nohome]
t 28 enabled=true
t 29
t 30 [apache-botsearch]
t 31 enabled=true
t 32
t 33 [apache-fakegooglebot]
t 34 enabled=true
t 35
t 36 [apache-modsecurity]
t 37 enabled=true
t 38
t 39 [apache-shellshock]
40 enabled=true
```

Рис. 2.5: Включение HTTP-jail-ов

После перезапуска Fail2ban журнал показал инициализацию каждого HTTP-jail-а, добавление их лог-файлов и успешный запуск.

```

2025-12-11 11:22:42,443 fail2ban.jail [19276]: INFO Creating new jail 'apache-shellshock'
2025-12-11 11:22:42,443 fail2ban.jail [19276]: INFO Jail 'apache-shellshock' uses pyinotify []
2025-12-11 11:22:42,444 fail2ban.jail [19276]: INFO Initiated 'pyinotify' backend
2025-12-11 11:22:42,445 fail2ban.filter [19276]: INFO maxRetry: 1
2025-12-11 11:22:42,445 fail2ban.filter [19276]: INFO findtime: 600
2025-12-11 11:22:42,445 fail2ban.actions [19276]: INFO banTime: 3600
2025-12-11 11:22:42,445 fail2ban.filter [19276]: INFO encoding: UTF-8
2025-12-11 11:22:42,445 fail2ban.filter [19276]: INFO Added logfile: '/var/log/httpd/error_log' (pos = 0, hash = 9c69734eeeeaac
574c9009e15dcc38ec56836f57c)
2025-12-11 11:22:42,445 fail2ban.filter [19276]: INFO Added logfile: '/var/log/httpd/ssl_error_log' (pos = 0, hash = 507f607fd
8b8e8943a69e8416d7ddc00d928b2c7)
2025-12-11 11:22:42,445 fail2ban.jail [19276]: INFO Creating new jail 'sshd-ddos'
2025-12-11 11:22:42,445 fail2ban.jail [19276]: INFO Jail 'sshd-ddos' uses pyinotify []
2025-12-11 11:22:42,446 fail2ban.jail [19276]: INFO Initiated 'pyinotify' backend
2025-12-11 11:22:42,446 fail2ban.filter [19276]: INFO maxLines: 1
2025-12-11 11:22:42,446 fail2ban.filter [19276]: INFO maxRetry: 5
2025-12-11 11:22:42,446 fail2ban.filter [19276]: INFO findtime: 600
2025-12-11 11:22:42,446 fail2ban.actions [19276]: INFO banTime: 3600
2025-12-11 11:22:42,446 fail2ban.filter [19276]: INFO encoding: UTF-8
2025-12-11 11:22:42,447 fail2ban.filtersystemd [19276]: INFO [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:22:42,447 fail2ban.jail [19276]: INFO Jail 'sshd' started
2025-12-11 11:22:42,447 fail2ban.jail [19276]: INFO Jail 'selinux-ssh' started
2025-12-11 11:22:42,448 fail2ban.jail [19276]: INFO Jail 'apache-auth' started
2025-12-11 11:22:42,450 fail2ban.jail [19276]: INFO Jail 'apache-badbots' started
2025-12-11 11:22:42,450 fail2ban.jail [19276]: INFO Jail 'apache-noscript' started
2025-12-11 11:22:42,450 fail2ban.jail [19276]: INFO Jail 'apache-overflows' started
2025-12-11 11:22:42,451 fail2ban.jail [19276]: INFO Jail 'apache-nohome' started
2025-12-11 11:22:42,451 fail2ban.jail [19276]: INFO Jail 'apache-botsearch' started
2025-12-11 11:22:42,452 fail2ban.jail [19276]: INFO Jail 'apache-fakegooglebot' started
2025-12-11 11:22:42,453 fail2ban.jail [19276]: INFO Jail 'apache-modsecurity' started
2025-12-11 11:22:42,453 fail2ban.jail [19276]: INFO Jail 'apache-shellshock' started
2025-12-11 11:22:42,454 fail2ban.jail [19276]: INFO Jail 'sshd-ddos' started

```

Рис. 2.6: Работа HTTP-jail-ов

## 2.1.5 Включение защиты почтовых сервисов

В локальной конфигурации были включены jail-ы для защиты почтовых сервисов: Postfix, Dovecot и других.

```
41
42 [postfix]
43 enabled=true
44
45 [postfix-rbl]
46 enabled=true
47
48 [dovecot]
49 enabled=true
50
51 [postfix-sasl]
52 enabled=true
```

Рис. 2.7: Включение защиты почтовых сервисов

После очередного перезапуска Fail2ban были созданы и запущены дополнительные jail-ы, что видно в логе:

- защита Postfix;
- защита SASL;
- защита Dovecot;
- активация RBL-фильтрации.

```

SYSTEMD_UNIT=postfix@.service
2025-12-11 11:24:36,669 fail2ban.filter      [19613]: INFO    maxRetry: 5
2025-12-11 11:24:36,669 fail2ban.filter      [19613]: INFO    findtime: 600
2025-12-11 11:24:36,669 fail2ban.actions     [19613]: INFO    banTime: 3600
2025-12-11 11:24:36,669 fail2ban.filter      [19613]: INFO    encoding: UTF-8
2025-12-11 11:24:36,669 fail2ban.jail       [19613]: INFO    Creating new jail 'sshd-ddos'
2025-12-11 11:24:36,669 fail2ban.jail       [19613]: INFO    Jail 'sshd-ddos' uses pyinotify {}
2025-12-11 11:24:36,670 fail2ban.jail       [19613]: INFO    Initiated 'pyinotify' backend
2025-12-11 11:24:36,670 fail2ban.filter      [19613]: INFO    maxlines: 1
2025-12-11 11:24:36,670 fail2ban.filter      [19613]: INFO    maxRetry: 5
2025-12-11 11:24:36,670 fail2ban.filter      [19613]: INFO    findtime: 600
2025-12-11 11:24:36,670 fail2ban.actions     [19613]: INFO    banTime: 3600
2025-12-11 11:24:36,670 fail2ban.filter      [19613]: INFO    encoding: UTF-8
2025-12-11 11:24:36,671 fail2ban.filtersystemd [19613]: INFO    [sshd] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,671 fail2ban.jail       [19613]: INFO    Jail 'sshd' started
2025-12-11 11:24:36,671 fail2ban.jail       [19613]: INFO    Jail 'selinux-ssh' started
2025-12-11 11:24:36,672 fail2ban.jail       [19613]: INFO    Jail 'apache-auth' started
2025-12-11 11:24:36,672 fail2ban.jail       [19613]: INFO    Jail 'apache-badbots' started
2025-12-11 11:24:36,672 fail2ban.jail       [19613]: INFO    Jail 'apache-noscript' started
2025-12-11 11:24:36,673 fail2ban.jail       [19613]: INFO    Jail 'apache-overflows' started
2025-12-11 11:24:36,673 fail2ban.jail       [19613]: INFO    Jail 'apache-nohome' started
2025-12-11 11:24:36,673 fail2ban.jail       [19613]: INFO    Jail 'apache-botsearch' started
2025-12-11 11:24:36,674 fail2ban.jail       [19613]: INFO    Jail 'apache-fakegooglebot' started
2025-12-11 11:24:36,674 fail2ban.jail       [19613]: INFO    Jail 'apache-modsecurity' started
2025-12-11 11:24:36,674 fail2ban.jail       [19613]: INFO    Jail 'apache-shellshock' started
2025-12-11 11:24:36,675 fail2ban.filtersystemd [19613]: INFO    [postfix-rbl] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,675 fail2ban.filtersystemd [19613]: INFO    [postfix] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,675 fail2ban.jail       [19613]: INFO    Jail 'postfix-rbl' started
2025-12-11 11:24:36,675 fail2ban.jail       [19613]: INFO    Jail 'dovecot' started
2025-12-11 11:24:36,676 fail2ban.filtersystemd [19613]: INFO    [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,676 fail2ban.jail       [19613]: INFO    Jail 'postfix-sasl' started
2025-12-11 11:24:36,676 fail2ban.filtersystemd [19613]: INFO    [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-11 11:24:36,676 fail2ban.jail       [19613]: INFO    Jail 'sshd-ddos' started

```

Рис. 2.8: Работа почтовых jail-ов

## 2.2 Проверка работы Fail2ban

Для проверки работоспособности Fail2ban был просмотрен общий статус сервиса.

В выводе отображается количество активных jail-ов и их список.

```

[root@server dgavdadaev.net server]# 
[root@server dgavdadaev.net server]# fail2ban-client status
Status
|- Number of jail:   16
`- Jail list:  apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript,
  apache-overflows, apache-shellshock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed:  0
| '- Journal matches: _SYSTEMD_UNIT:sshd.service + _COMM:sshd + _COMM:sshd-session
`- Actions
  |- Currently banned: 0
  | |- Total banned:  0
  | '- Banned IP list:
[root@server dgavdadaev.net server]# fail2ban-client set sshd maxretry 2
2
[root@server dgavdadaev.net server]#

```

Рис. 2.9: Общий статус Fail2ban

Был просмотрен статус jail-a sshd, где отображаются:

- количество неудачных попыток входа;
- количество заблокированных IP-адресов;

- список заблокированных адресов.

```
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
  `- Banned IP list: 192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
  `- Banned IP list:
[root@server.dgavdadaev.net server]#
```

Рис. 2.10: Статус защиты SSH

Для усиления защиты была установлена величина максимального количества ошибок при попытке входа:

```
[root@server.dgavdadaev.net server]#
[root@server.dgavdadaev.net server]# fail2ban-client status
Status
|- Number of jail: 16
`- Jail list: apache-auth, apache-badbots, apache-botsearch, apache-fakegooglebot, apache-modsecurity, apache-nohome, apache-noscript,
apache-overflows, apache-shells Shock, dovecot, postfix, postfix-rbl, postfix-sasl, selinux-ssh, sshd, sshd-ddos
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 0
  `- Banned IP list:
[root@server.dgavdadaev.net server]# fail2ban-client set sshd maxretry 2
2
[root@server.dgavdadaev.net server]#
```

Рис. 2.11: Установка maxretry

После нескольких неудачных попыток входа с клиента Fail2ban заблокировал адрес, что подтверждается обновлённым статусом jail-a.

```

[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
  `- Banned IP list: 192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
  `- Banned IP list:
[root@server.dgavdadaev.net server]#

```

Рис. 2.12: Блокировка IP после неудачных попыток входа

IP-адрес клиента был успешно разблокирован с помощью соответствующей команды.

После выполнения команды статус jail-а обновился, и количество текущих блокировок стало равно нулю.

```

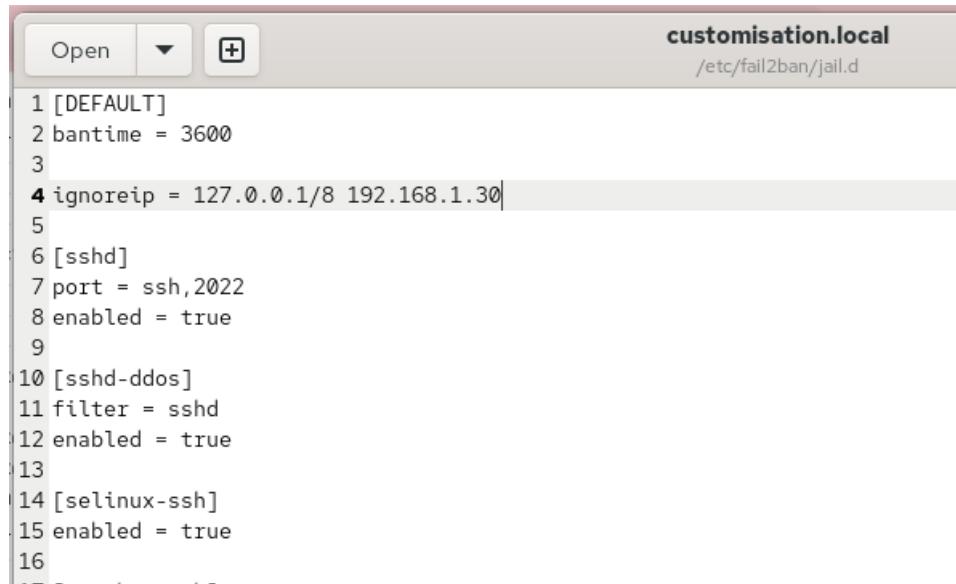
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 1
  |- Total banned: 1
  `- Banned IP list: 192.168.1.30
[root@server.dgavdadaev.net server]# fail2ban-client set sshd unbanip 192.168.1.30
1
[root@server.dgavdadaev.net server]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 3
| `- Journal matches: _SYSTEMD_UNIT=sshd.service + _COMM=sshd + _COMM=sshd-session
`- Actions
  |- Currently banned: 0
  |- Total banned: 1
  `- Banned IP list:
[root@server.dgavdadaev.net server]#

```

Рис. 2.13: Разблокировка адреса клиента

В локальную конфигурацию Fail2ban было добавлено исключение, запрещающее блокировать определённый IP-адрес.

Изменение внесено в раздел [DEFAULT] файла локальной конфигурации.



```
customisation.local
/etc/fail2ban/jail.d

1 [DEFAULT]
2 bantime = 3600
3
4 ignoreip = 127.0.0.1/8 192.168.1.30
5
6 [sshd]
7 port = ssh,2022
8 enabled = true
9
10 [sshd-ddos]
11 filter = sshd
12 enabled = true
13
14 [selinux-ssh]
15 enabled = true
16
```

Рис. 2.14: Добавление ignoreip

После перезапуска Fail2ban в журнале появилось подтверждение, что указанный IP теперь игнорируется.

```
2025-12-11 11:28:16,340 fail2ban.filtersystemd [20215]: INFO [dovecot] Jail is in operation now (process new journal entries)
2025-12-11 11:28:16,340 fail2ban.filtersystemd [20215]: INFO [postfix-sasl] Jail is in operation now (process new journal entries)
2025-12-11 11:28:16,340 fail2ban.jail [20215]: INFO Jail 'postfix-sasl' started
2025-12-11 11:28:16,341 fail2ban.jail [20215]: INFO Jail 'sshd-ddos' started

2025-12-11 11:28:27,806 fail2ban.filter [20215]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:28:32,509 fail2ban.filter [20215]: INFO [sshd] Ignore 192.168.1.30 by ip
2025-12-11 11:28:36,800 fail2ban.filter [20215]: INFO [sshd] Ignore 192.168.1.30 by ip
```

Рис. 2.15: Fail2ban игнорирует IP-адрес клиента

После внесения IP в ignoreip повторная попытка входа с неправильным паролем не привела к блокировке, что подтверждается отсутствием записей о бane в статусе jail-a sshd.

## 2.3 Внесение изменений во внутреннее окружение виртуальной машины

На виртуальной машине были созданы каталоги для хранения кастомных конфигураций Fail2ban, которые используются при provisioning'e Vagrant.

```
[root@server.dgavdadaev.net server]#  
[root@server.dgavdadaev.net server]#  
[root@server.dgavdadaev.net server]# cd /vagrant/provision/server/  
[root@server.dgavdadaev.net server]# mkdir -p /vagrant/provision/server/protect/etc/fail2ban/jail.d  
[root@server.dgavdadaev.net server]# cp -R /etc/fail2ban/jail.d/customisation.local /vagrant/provision/server/protect/etc/fail2ban/jail.d  
/[root@server.dgavdadaev.net server]# touch protect.sh  
[root@server.dgavdadaev.net server]#
```

Рис. 2.16: Создание каталогов и копирование конфигурации

В каталоге `/vagrant/provision/server` был создан исполняемый файл `protect.sh`, содержащий:

- установку Fail2ban;
- копирование заранее подготовленных конфигураций;
- восстановление контекстов SELinux;
- запуск и включение Fail2ban в автозагрузку.



```
#!/bin/bash  
echo "Provisioning script $0"  
echo "Install needed packages"  
dnf -y install fail2ban  
echo "Copy configuration files"  
cp -R /vagrant/provision/server/protect/etc/* /etc  
restorecon -vR /etc  
echo "Start fail2ban service"  
systemctl enable fail2ban  
systemctl start fail2ban
```

Рис. 2.17: Скрипт `protect.sh`

# **3 Итоги**

## **3.1 Вывод**

Fail2ban обеспечивает автоматическую защиту сервера, анализируя журналы и блокируя источники подозрительной активности. В ходе работы были настроены jail-ы для SSH, веб- и почтовых служб, проверена блокировка и разблокировка IP, добавлены исключения, а также подготовлен provisioning-скрипт для автоматизации конфигурации. Система функционирует корректно и эффективно повышает безопасность сервера.

## **3.2 Контрольные вопросы**

**1. Поясните принцип работы Fail2ban.** Fail2ban анализирует журналы системных сервисов и отслеживает повторяющиеся ошибки (например, неудачные попытки входа). При превышении установленного лимита программа динамически добавляет правила в брандмауэр и блокирует IP-адрес нарушителя на заданное время.

**2. Настройки какого файла более приоритетны: jail.conf или jail.local?** Наиболее приоритетны настройки **jail.local** – именно этот файл предназначен для переопределения значений по умолчанию, указанных в *jail.conf*.

**3. Как настроить оповещение администратора при срабатывании Fail2ban?** В секции действий Fail2ban можно указать отправку email-сообщений. Для этого выбирают **action**, поддерживающий уведомления, например:

- `action = %(action_mwl)s`

Также необходимо корректно настроить локальную почтовую систему, чтобы Fail2ban мог отправлять письма.

**4. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к веб-службе.** Основные параметры для веб-служб включают:

- указание соответствующих фильтров для Apache/Nginx;
- выбор лог-файлов, которые должны анализироваться;
- активацию или деактивацию нужных jail-ов;
- настройку временных интервалов (findtime, bantime);
- определение лимита ошибок (maxretry).

Эти параметры задают общие правила мониторинга веб-сервера и его реакцию на подозрительные запросы.

**5. Поясните построчно настройки по умолчанию в конфигурационном файле `/etc/fail2ban/jail.conf`, относящиеся к почтовой службе.** Стандартные секции для почтовых служб включают:

- выбор фильтра (например, postfix, dovecot);
- включение или отключение конкретного jail-a;
- указание логов почтовых сервисов;
- определение временных интервалов и числа попыток;
- выбор действий при обнаружении попыток взлома.

Эти настройки позволяют контролировать работу SMTP/IMAP/POP сервисов и блокировать попытки подбора паролей.

**6. Какие действия может выполнять Fail2ban при обнаружении атакующего IP-адреса? Где посмотреть описание действий?** Fail2ban может:

- блокировать IP через firewall;

- отправлять уведомления администратору;
- выполнять пользовательские скрипты;
- объединять несколько действий в один сценарий.

Описание действий находится в директории:

- `/etc/fail2ban/action.d/`

Каждый файл описывает конкретное действие и может использоваться в настройках jail-ов.

**7. Как получить список действующих правил Fail2ban?** Получить список активных jail-ов можно с помощью:

- `fail2ban-client status`

Этот вывод включает общее количество jail-ов и их названия.

**8. Как получить статистику заблокированных Fail2ban адресов?** Используют команду:

- `fail2ban-client status <jail>`

Она показывает:

- число текущих блокировок;
- общее количество заблокированных IP;
- список заблокированных адресов.

**9. Как разблокировать IP-адрес?** Для снятия блокировки выполняется команда:

- `fail2ban-client set <jail> unbanip <IP>`

Она удаляет IP из списка заблокированных и снимает правило из брандмауэра.